ELECTRONIC PAYMENT AUTHORISATION

Background to the Invention

This invention relates to a method and apparatus for authorising electronic payments.

The object of the present invention is to provide a method for enabling customers to make electronic payments to suppliers of goods and services, in a secure and efficient manner.

Summary of the Invention

According to the invention, in a method for authorising an electronic payment:
(a) details of a proposed transaction are sent to an authorisation computer, the details including an identification of a customer, a monetary amount to be paid by the customer, and an identification of a payee to whom the payment is to be made;
(b) the authorisation computer sends a message to a telephone number associated with the customer, the message containing details of the proposed transaction and requesting the customer to confirm payment by supplying a specified, randomly selected, sub-set of characters of a multi-character pass phrase associated with the customer;
(c) when the customer replies to the message by supplying the specified sub-set of characters, the authorisation computer checks that the characters are correct and, if so, authorises transfer of the specified amount from the customer's account to the payee's account.

Description of an Embodiment of the Invention

One embodiment of the invention will now be described by way of example with reference to the accompanying drawing, which is a

schematic block diagram of a computer system for authorising electronic payments.

The drawing shows a e-commerce (electronic commerce) server computer 10, which hosts an on-line electronic shopping website. The website can be accessed over the Internet 11, from a customer's personal computer 12, using conventional web browser software. It is also assumed that each customer has a mobile phone 13 which is capable of sending and receiving Short Message Service (SMS) text messages.

The drawing also shows a mobile payment system (MPS) server computer 14, and a banking system computer 15, both of which operate inside a banking system firewall 16. The MPS computer 14 provides an electronic payments service for authorising electronic payments from customers to suppliers of goods and services in a secure manner.

Customers who wish to use the electronic payments service must first register with the service as will be described. The MPS server has a secure database 17, which holds the following details for each customer registered with it: mobile payment ID; name and address; details of account from which payments are to be made; mobile telephone number; and pass phrase.

The e-commerce server 10 operates in a conventional manner, allowing the customer to view details of goods for sale, and to select items to place in an electronic "shopping basket". when the customer has selected all the desired items, the customer can proceed to a checkout screen, which lists all the items in the basket and the total payment due. The checkout screen offers the customer a number of options for how the customer wishes to pay. One of the options is "Mobile payment".

If the customer selects the "Mobile payment" option, the e-commerce server 10 requests the customer to enter their mobile

payment ID. It then sends an encrypted message to the MPS server. This message contains details of the transaction, including the customer's mobile payment ID, the amount to be paid by the customer, and the identity of the payee to whom payment is to be made.

When the MPS server 14 receives this message, it retrieves the customer's details from its secure database. It then sends an SMS message to the customer's mobile phone, using the number obtained from the database. This message contains the amount of payment requested, the identity of the payee, and specifies three randomly selected characters of the customer's pass phrase that the customer should supply to authorise the payment. For example, the SMS message might read:

> "ShopX requests you to pay £99. Authorise with a reply of letters 4, 7 and 13 of your pass phrase."

(SMS messages are limited to 160 characters).

When the customer receives this message, he or she selects "Reply", and keys in the requested three characters, using the standard telephone keypad lettering. For example, letters "a", "b" and "c" are keyed in by pressing key "2", and so on. The customer then presses "Send" to send the reply message back to the MPS server.

When the MPS server 14 receives the reply message, it checks the three characters against the corresponding three characters of the customer's pass phrase. If they are equal, the MPS computer sends a message to the banking system computer 15, requesting it to transfer the desired amount from the customer's account to the payee's account. Finally, the MPS server sends an encrypted message to the e-commerce server, informing it that the transaction is complete. The e-commerce server will then display the normal "transaction complete" screen to the customer.

If, on the other hand, the three characters in the reply message are not equal to the corresponding three characters of the customer's pass phrase, or if a reply message is not received within a predetermined time, the MPS server sends an encrypted message to the e-commerce server, informing it that the transaction has failed.

As mentioned above, customers who wish to use the electronic payments service must first register with the service. Conveniently, registration is performed on-line, using a web-based system.

The registration process first requires the customer to provide his or her name, address, mobile telephone number, and details of the account from which payments are to be made - this will normally be a credit card or debit card account.

The registration process then assigns a mobile payment ID to the customer. This is a unique membership number that identifies the customer to the service. As described above, this number is required to be quoted by the payee in order for the MPS server to identify the subscriber and authorise payment.

The registration process then invites the customer to select a secret pass phrase, preferably at least 14 characters long. Selecting an appropriate pass phrase, which is in reality a long PIN, is an important part of the registration process. The user is guided to select a phrase of meaning only to them, with a strong image associated with it: for example, the second line of a favourite poem. Such a phrase would be easily remembered, and it is also easy for the customer to mentally count through the phrase to find the requested characters.

Preferably, the pass phrase consists solely of the characters "a" to "z" corresponding to keys "2" to "9" on the standard telephone keypad. The keys for "space", "*" and "#" are not

used, since they are frequently confused by non-computer-literate people.

The registration system then makes a test run to validate the account, by sending a test message to the customer's mobile phone and receiving the customer's reply. This is needed to ensure that the user has correctly entered the phone number and has remembered the pass phrase, and to demonstrate the messages in a non-threatening environment. If the user gets anything wrong at this stage the system can explain more, check the details and re-run the test.

It can be seen that the method described above ensures that only a portion of the pass phrase is transmitted during each individual transaction. Thus, even if the messages are intercepted, the pass phrase is not revealed, and messages cannot simply be replayed since a different random selection of characters will be requested for each transaction.

It should also be noted that the method described above ensures that the payee does not learn the customer's account details, such as credit card numbers. These details are required only by the MPS server. This introduces an extra safety factor for the customer.

Some possible modifications

It will be appreciated that many modifications may be made to the system described above without departing from the scope of the present invention.

For example, instead of using SMS messages, the MPS server may use an interactive voice response (IVR) system. In this case, after retrieving the customer's details from the database, the MPS server would make an IVR call to the user's phone, indicating the amount of payment requested, the identity of the

payee, and specifying three randomly selected characters of the customer's pass phrase that the customer should supply to authorise the payment. For example, the IVR message might say: "ShopX has requested payment of £99. To authorise the payment, please type characters 4, 7 and 13 of your pass phrase now." The customer would then key in the requested characters, and after a short pause would hear a confirmation message, such as: "Thank you, you have authorised the payment of £99 to ShopX" following which the IVR system would hang up.

Because IVR is a voice channel it is possible to add a further level of security by using voice print analysis. Such a system would work by asking the customer to say a particular word after the requested characters of the pass phrase had been correctly transmitted. The word would then be compared with a sample of the word recorded by the customer during the registration process.

Although the example described above was for payments to an on-line shopping service, the invention could also be used for authorising payments at a POS (point-of-sale) terminal, e.g. in a retail store, or restaurant, or at a vending machine. In addition to payment for goods, the invention can equally be used to pay for services, such as car parking and taxi or other fares. It can also be used to top-up pre-payment accounts, for example for pre-pay mobile phones.

The system described above could also be extended to cover sending of a P2P (person to person) payment by one customer to another subscriber to the mobile payment system.

In another possible modification, the customer's account details are not held on the MPS server. Instead, the MPS server would use the customer's Mobile Payment ID to identify the customer to the Bank computer when requesting a transfer.